

Title (en)

Cryptographic method and apparatus

Title (de)

Kryptografisches Verfahren und Gerät

Title (fr)

Procédé et appareil cryptographique

Publication

EP 1605626 B1 20071226 (EN)

Application

EP 05104894 A 20050606

Priority

GB 0413056 A 20040611

Abstract (en)

[origin: EP1605626A1] A cryptographic method and apparatus is provided in which a first party (A) receives and modifies a public key (p, g, y) for which there exists a corresponding private key (x) held by a second party (TA). The public key is modified by exponentiating at least one element (y) of the received public key using as exponent a hash of a string (STR) that comprises information concerning at least one action to be taken by the second party (TA). The string (STR) is made available to the second party (TA) to enable the latter to modify its private key to compliment the modified public key. In a preferred embodiment, the method and apparatus are applied to the use of the ElGamal encryption/decryption scheme, with the second party (TA) acting as a trusted authority that only releases the decrypted message to a third party (B) if the latter satisfies an identity condition specified in the string. For privacy reasons, the third party (B) may blind the encrypted message before passing it to the second party for decryption.

IPC 8 full level

H04L 9/30 (2006.01); **H04L 29/06** (2006.01)

CPC (source: EP GB US)

H04L 9/0643 (2013.01 - GB); **H04L 9/3013** (2013.01 - EP GB US); **H04L 9/3066** (2013.01 - GB); **H04L 9/321** (2013.01 - EP US); **H04L 9/3236** (2013.01 - GB); **H04L 2209/046** (2013.01 - EP US)

Designated contracting state (EPC)

DE FR GB

DOCDB simple family (publication)

EP 1605626 A1 20051214; **EP 1605626 B1 20071226**; DE 602005003984 D1 20080207; DE 602005003984 T2 20081218; GB 0413056 D0 20040714; GB 2415112 A 20051214; GB 2415112 B 20070425; US 2005276414 A1 20051215; US 7801302 B2 20100921

DOCDB simple family (application)

EP 05104894 A 20050606; DE 602005003984 T 20050606; GB 0413056 A 20040611; US 15062305 A 20050610